Remarks

This communication is considered fully responsive to the second Office Action mailed July 30, 2007. Claims 1-20 were examined. Claims 1-20 stand rejected. Claims 1, 2, 5-8, 11-16, 19 and 20 have been amended and claims 17 and 18 have been canceled; claims 3, 4, 9 and 10 remain unchanged. Reexamination and reconsideration of claims 1-16, 19 and 20 are respectfully requested.

Claim Rejections - 35 U.S.C. 101

The Office Action rejected claims 6-10 under 35 U.S.C. 101 as being directed to non-statutory subject matter. The Applicant disagrees with the rejection. However, in order to advance prosecution of the application, paragraph [0006] has been amended by deleting the sentence in question. No new matter has been added. The Applicant respectfully requests that the rejection under §101 be reconsidered and withdrawn.

Claim Rejections - 35 U.S.C. 102(b)

The Office Action rejected claims 1-15 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,199,113 to Alegre (hereinafter referred to as "Alegre"). The Applicant respectfully traverses this rejection. The claims have been amended to more clearly recite the interaction of the security host with two components, a remote client and a system host. In the claimed invention, an access request from the remote client is transmitted not directly to the system host but to the security host. In the exemplary networked computing system illustrated in FIG. 1 and described in the Specification (beginning in paragraph [0019], the security host of claim 11 is separate from the system host 140. Thus, the remote client is unable to even attempt to establish a communications link with the system host until the separate security host verifies that the user at the remote host is authorized to access the system host. Only then will the remote client receive the network address of the system host. After the remote client attempts to access the system host, the system host requests verification from the security host that the remote client is authorized to access the system host. When the system host receives such verification from the security host, the remote client is allowed to access the system host.

Alegre fails to teach at least these recitations and, as illustrated in FIG. 2, is far more complicated than the claimed invention, as illustrated in FIG. 2 of the present

application. In contrast to the claimed invention, in which all security (authorization and verification) takes place in a security host connected to the network, Alegre teaches that security requires several separate servers (database server, authentication server and key server) located behind a firewall from the web host which, in turn is behind a firewall from the client browser. Thus, the web host of Alegre serves merely as an intermediate component between the client browser, the security servers and the trusted network. Only after the initial authentication of the client browser has been performed is the client browser presented with a selection of resources which are available to the client browser. The user, through the client browser, then selects the desired resource to access. In response to the selection, the web browser sends the selection to an access server which initiates a verification of the client browser. Communications between the client browser and the access server on the trusted network, even after authentication and verification, passes through the web host (see, for example, column 4, lines 65-67, of Alegre).

In the claimed invention, the initial request sent by the user at the remote client specifies the desired system host, even before the remote client is provided by the security host with security credentials. The remote client then attempts to access the system host directly, not through the security host. In response, the system host verifies through the security host that the remote client is authorized to access the system host. Following verification by the security host, the system host grants direct access to the remote client, without having to pass communications through the security host.

Thus, although the Office Action appears to equate the web host of Alegre with the claimed security host, the web host in fact merely acts as a conduit between the client browser and both the security components and the desired resource.

The remarks in the preceding paragraphs are equally applicable to the rejection of all claims under §102. Consequently, Alegre does not anticipate amended claims 1-15 and withdrawal of the §102 rejection is respectfully requested.

Claim Rejections - 35 U.S.C. 103(a)

The Office Action rejected claims 16-20 under 35 U.S.C. 103(a) as being unpatentable over Alegre in view of U.S. Patent No. 6,487,457 to Hull (hereinafter referred to as "Hull"). Applicant respectfully traverses this rejection.

Claims 16, 19 and 20 depend from claim 11 (claims 17 and 18 having been cancelled), which is believed to be allowable. Because Alegre does not disclose or suggest all of the elements of claim 11, the combination of Hull with Alegre would not result in the invention recited in claims 16, 19 or 20. Therefore, claims 16, 19 and 20 are also believed to be allowable for at least the same reasons as claim 11 and withdrawal of the §103 rejection is respectfully requested.

Conclusion

For the foregoing reasons, the pending claims are believed to be allowable, the Application is believed to be in condition for allowance and the Applicant respectfully requests that a timely Notice of Allowance be issued in this matter. The Examiner is encouraged to contact the undersigned by telephone if a conversation would expedite prosecution of this case.

Respectfully Submitted,

/Mark D. Trenner/

Dated: October 29, 2007 By: _____

Mark D. Trenner
Reg. No. 43,961
(720) 221-3708